A VIEW FROM CONGRESS ON FISMA

Presentation to the Information Security and Privacy Advisory Board

September 4, 2008

George Washington University, Cafritz Conference Center

Erik Hopkins

Professional Staff

Subcommittee on Federal Financial Management,

Government Information, Federal Services,

And International Security

Current FISMA “Framework”

- Agency head responsible for overall information security
- Business owners responsible for assessing and implementing information security
- CIO asserts compliance of business owners
- Independent Evaluation tests CIO assertion
- Congress receives reports from OMB and

FISMA Success Since 2002

- Comprehensive IT governance structure
- Increased focus on information security by senior agency officials
- Directed resources and budget to the CIO office
- Increased percentage of Certification and Accreditation government-wide
- Increased accountability with CIO office

Information Environment Since 2002

- Exponential increase in the number and severity of external attacks both reported and unreported
- Increase in number of insider threats both intentional and unintentional
- Increased sophistication of attacks through means such as social engineering and vulnerable supply chains
- Increased use of mobile devices, uncontrolled points of access, and increasing interconnectivity

Information Security Improvements 2002 versus 2008

- Are we “more secure” now than we were 6 years ago?
- How do we measure “security?”
- How do we prioritize resources to face the evolving threat?
- How can Congress hold agencies accountable?

Problems with FISMA Implementation

- There is a lack of outcome-oriented measures that can be compared over time
- There is little focus on the ability to monitor, respond, and mitigate security incidences
- There is no way to accurately compare security between agencies
- Congress has little insight into agency information security
- Agencies prioritize their own resources based upon Congressional and OMB attention

How Can We Improve the Information Security Environment

- Improve information security measures
  - Outcome/effectiveness-oriented
  - Measure progress over time
  - Measure ROI
- Prioritize and direct resources against greatest threats
- Incentivize open collaboration
- Treat security holistically- not system by system/ agency by agency

Possible Solutions

- Develop and implement standardized information security measures
- Increase visibility and authority of CIO/CISO over information security
- Standardize independent evaluation
- Breakdown artificial organizational boundaries
- Test agency information security based on intelligence
- Provide decision-makers holistic view of security government-wide.

Partners for Success

- The educated individual
- The responsible business owner
- The empowered CISO
- The informed agency head
- An educated Executive and Legislative branch

Legislative Aspirations

- Increase the resources, quality, and responsibility of the CISOs
- Shift the security paradigm
- Standardize the independent evaluation
- Create a central forum composed of those who are facing the threats every day
- Supplement the CIO assertion and IG evaluation with an operational evaluation
- Require that network service providers and COTS are held to government standards

Questions